

CLAIMS

What is claimed is:

1. A method of tracking changes to a customer system in a managed hosting environment comprising:
performing periodic audits of the customer system by executing an agent program that is resident on the customer system and that collects information to be transferred to an application server connected with the customer system via a network; and
determining whether changes have been made to the software of the customer system by monitoring said information on the application server.
2. The method of claim 1, wherein said performing periodic audits comprises:
reading a predetermined set of information from the customer system;
generating a set of change data on the application server indicating changes that have been made to the customer system since the last periodic audit by comparing the predetermined set of information to a predetermined set of information recorded during a previous audit; and
storing said change data on a database server connected with the application server via a network.
3. The method of claim 2, wherein said predetermined set of information comprises operating system files, file system, registry, and application software files of the customer system.

4. The method of claim 2, wherein said change data is compressed and encrypted prior to being stored.
5. The method of claim 1, further comprising:
 - checking out the customer system from the application server, thereby allowing the application server to make changes to the software of the customer system;
 - suspending periodic auditing;
 - taking a first snapshot of the customer system;
 - checking in the customer system when changes to the software of the customer system have been completed;
 - taking a second snapshot of the customer system;
 - generating change data on the application server by comparing the first snapshot and the second snapshot;
 - storing said change data on a database server connected with the application server via a network; and
 - resuming periodic auditing.
6. The method of claim 5, wherein said first and second snapshots comprise operating system files, file system, registry, and application software files of the customer system.
7. The method of claim 5, wherein said change data is compressed and encrypted prior to being stored.

- 1 4 2
8. The method of claim 2, further comprising:
reading a set of rules from a database server connected with the application server via a
network;
applying the set of rules to the change data to determine whether any of said set of rules has
been violated; and
responsive to a violation of any of said set of rules, taking an action associated with a rule
violated.
9. The method of claim 8, wherein said rules are stored on the database server.
10. A system comprising:
a customer system available to a customer in a managed hosting server;
an application server connected with said customer system via a network to generate change
data based on audit data or snapshot data read from the customer system;
a database server connected with said application server via a network to maintain a database
of change data generated by the application server;
a report server connected with said database server via a network to generate reports based
on the changed data stored on the database server;
a command center connected with said application server and said report server via a network
to retrieve reports from the report server.
11. The system of claim 10, wherein said customer system executes an agent application that
periodically collects audit data and collects snapshot data responsive to a request from the
application server.

12. The system of claim 10, wherein said application sever is further configured to:
read a predetermined set of information from the customer system;
generate a set of change data indicating changes that have been made to the customer system
since the last periodic audit by comparing the predetermined set of information to a
predetermined set of information recorded during a previous audit; and
store said change data on the database server.
13. The system of claim 12, wherein said application server compresses and encrypts said change
data before storing the change data on the database server.
14. The system of claim 10, wherein said application server is further configured to:
check out the customer system, thereby allowing the application server to make changes to
the software of the customer system;
suspend periodic auditing;
take a first snapshot of the customer system;
check in the customer system when changes to the software of the customer system have
been completed;
take a second snapshot of the customer system;
generate change data by comparing the first snapshot and the second snapshot;
store said change data on the database server; and
resume periodic auditing.
15. A machine-readable medium having stored thereon data representing sequences of
instructions, said sequences of instructions which, when executed by a processor, cause said
processor to:

perform periodic audits of the customer system by executing an agent program that is resident on the customer system and that collects information to be transferred to an application server connected with the customer server via a network; and determine whether changes have been made to the software of the customer system by monitoring said information on the application server.

16. The machine-readable medium of claim 15, wherein said performing periodic audits comprises:
- reading a predetermined set of information from the customer system;
 - generating a set of change data on the application server indicating changes that have been made to the customer system since the last periodic audit by comparing the predetermined set of information to a predetermined set of information recorded during a previous audit; and
 - storing said change data on a database server connected with the application server via a network.
17. The machine-readable medium of claim 16, wherein said predetermined set of information comprises operating system files, file system, registry, and application software files of the customer system.
18. The machine-readable medium of claim 16, wherein said change data is compressed and encrypted prior to being stored.

19. The machine-readable medium of claim 15, further comprising:
- checking out the customer system from the application server, thereby allowing the
- application server to make changes to the software of the customer system;
- suspending periodic auditing;
- taking a first snapshot of the customer system;
- checking in the customer system when changes to the software of the customer system have
- been completed;
- taking a second snapshot of the customer system;
- generating change data on the application server by comparing the first snapshot and the
- second snapshot;
- storing said change data on a database server connected with the application server via a
- network; and
- resuming periodic auditing.
20. The machine-readable medium of claim 19, wherein said first and second snapshots comprise
- operating system files, file system, registry, and application software files of the customer
- system.
21. The machine-readable medium of claim 19, wherein said change data is compressed and
- encrypted prior to being stored.
22. The machine-readable medium of claim 16, further comprising:
- reading a set of rules from a database server connected with the application server via a
- network;

applying the set of rules to the change data to determine whether any of said set of rules has been violated; and responsive to a violation of any of said set of rules, taking an action associated with a rule violated.

23. The machine-readable medium of claim 22, wherein said rules are stored on the database server.

11/11/2011 11:11:11 AM